Najpopularniejsze zagrożenia w sieci

W codziennym korzystaniu z Internetu najczęściej można spotkać się z następującymi zagrożeniami:

- **Phishing (wyłudzanie danych): Oszustwo polegające na podszywaniu się pod znane instytucje (banki, urzędy, firmy kurierskie, dostawców energii) za pomocą wiadomości e-mail lub SMS (Smishing). Celem oszustów jest skłonienie ofiary do kliknięcia w link i podania loginów, haseł lub danych karty płatniczej na fałszywej stronie.**
- **Vishing (wyłudzanie przez telefon): Oszustwo telefoniczne, w którym przestępca podszywa się np. pod pracownika banku, policjanta lub urzędnika, próbując wywrzeć presję czasu i skłonić do wykonania przelewu lub zainstalowania aplikacji do zdalnego pulpitu.**
- **Złośliwe oprogramowanie (Malware): Wirusy, trojany czy oprogramowanie szpiegujące instalowane nieświadomie przez użytkownika (np. poprzez pobranie zainfekowanego załącznika). Szczególnie groźne jest oprogramowanie typu Ransomware, które szyfruje pliki na dysku i żąda okupu za ich odblokowanie.**
- **Kradzież tożsamości: Przejęcie danych osobowych (np. PESEL, serii i numeru dowodu osobistego) w celu wyłudzenia kredytów, pożyczek lub założenia fałszywych kont bankowych.**
- **Słabe lub powtarzające się hasła: Używanie tego samego hasła w wielu serwisach ułatwia przestępcom przejęcie dostępu do wszystkich kont (np. poczty e-mail, mediów społecznościowych i bankowości) po wycieku danych z jednego portalu.**

Jak się chronić? Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz. Haseł do systemów informatycznych nie zdradzaj nigdy i nikomu.

Podstawowym elementem bezpieczeństwa w sieci Internet jest zastosowanie zasady ograniczonego zaufania i podwyższonej ostrożności. Dlatego też zachęca się do:

- **używania oprogramowania antywirusowego i zapory sieciowej (firewall);**
- **korzystania wyłącznie z legalnego i aktualnego oprogramowania;**
- **unikania korzystania z sieci publicznych, w przypadku logowania się do systemów informatycznych zawierających cenne dane lub dane podlegające ochronie;**
- **regularnej aktualizacji oprogramowania oraz bazy danych wirusów;**
- **nie otwierania podejrzanych e-maili oraz ich załączników;**
- **nie korzystania ze stron WWW, które nie mają ważnego certyfikatu (np. brak protokołu https);**
- **nie pozostawiania swoich danych osobowych w niesprawdzonych serwisach i na stronach internetowych;**
- **czytanie zawsze dokładnie Regulaminów i Polityk serwisów WWW oraz weryfikowanie zakresu wyrażanych zgód;**
- **nie wysyłania e-mailem poufnych danych bez ich szyfrowania.**

Pamiętaj, że placówka medyczna, bank czy Urząd, nie wysyła e-maili do swoich pacjentów/klientów/interesantów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji!

Gdzie szukać pomocy i jak zgłosić incydent?

Jeśli podejrzewasz, że padłeś ofiarą cyberprzestępstwa lub otrzymałeś podejrzaną wiadomość, zgłoś to natychmiast odpowiednim służbom:

- **Zgłoszenia w aplikacji mobilnej: Skorzystaj z funkcji „Bezpiecznie w sieci" w aplikacji mObywatel, aby szybko i wygodnie zgłosić podejrzaną stronę, e-mail lub oszustwo telefoniczne.**
- **Kradzież pieniędzy lub tożsamości: W przypadku wyłudzenia środków finansowych lub kradzieży danych osobowych, niezwłocznie poinformuj swój bank (w celu zablokowania kart/kont) oraz zgłoś sprawę na najbliższym komisariacie Policji.**

Przydatne źródła i poradniki (baza wiedzy)

Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym:
www.cert.pl/ouch/
Poradniki na witrynie internetowej Ministerstwa Cyfryzacji, które przybliżają problematykę cyberbezpieczeństwa
www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
Publikacje z zakresu cyberbezpieczeństwa:
www.cert.pl/